Journal of Information Engineering and Applications
ISSN 2224-5782 (print) ISSN 2225-0506 (online) DOI: 10.7176/JIEA
Vol.9, No.5, 2019
www.iiste.org

Monitoring IT and Internet Usage of Employees for Sustainable Economic Development in Nigeria: Legal and Ethical Issues.

Felix. C. Aguboshim[1] Joy. E. Ezeife[2] Irene. N. Ezeasomba[3]
1. Principal Lecturer at Federal Polytechnic Oko, Department of Computer Science, Oko, Nigeria
2. Lecturer, at Federal Polytechnic Oko, Department of Computer Science, Oko, Nigeria
3. Principal Lecturer at Federal Polytechnic Oko, Department of Computer Science, Oko, Nigeria

Abstract
Globally, organization system resources: hardware, software, data, and communication lines and networks are now handled with better interconnected and interdependent facilities because internet connectivity is widely integrated into ambient or ubiquitous environments through intuitive interfaces or "smart" interactions. Organization enterprises are increasingly becoming competitive, with widespread cyberloafing and lawsuits. Through IT and Internet usage, employees may compromise an organization's confidential information, deliberately or inadvertently. Such concerns prompt companies to introduce employee monitoring to preserve the integrity, availability, and confidentiality of system resources, track employee performance, avoid legal liability, protect trade secrets, and address security concerns. Despite these laudable benefits, employees feel that monitoring is an invasion of their privacy rights. For this study, organizational ethics and major ethical principles of respect for persons, beneficence, and justice representing the key ethical concerns for human subject protection in research were fully adopted as identified in The Belmont Report of 1979. In this study, the authors explored a narrative review, analysis, and synthesis of prior researches that focused on monitoring of employee IT and Internet usage. The authors also extracted peer-reviewed articles within the last five years from electronic databases, using some search keys such as "employee monitoring", "legal and ethical issues", "impact of employee monitoring on economic sustainability", etc. The result of this study revealed that developing an acceptable monitoring policy will keep both employer and employee on the same page as to what is acceptable in the workplace along with what isn't. This result may further explain the need for employee monitoring, address the legal and ethical issues involved when monitoring employees in a work environment, and provide strategies and practices for acceptable monitoring policy for improved organizational performance and sustainable economic development.
Keywords: Employee Monitoring, Legal and Ethical Issues, IT and Internet Usage. Economic Sustainability.
DOI: 10.7176/JIEA/9-5-03
Publication date: August 31st 2019

1. Introduction

The Internet has become a major source of communication both within and outside organizations. The internet is a global network communications incorporating private, public, business, academic and government networks that are connected by guided, wireless, and fiber-optic technologies. "Internet is a global system of interconnected networks of computers and other communication devices that use standardized communication protocols to link devices worldwide to provide a variety of information and communication services" (NITDA, 2019, p. 6). The Internet as a global village for communication of email, web-enabled audio/video conferencing services, online movies and gaming, data transfers/file sharing, instant messaging, internet forum, social networking, online shopping for musical studio and pornographic materials amongst other things. Employees in particular use the internet extensively for communication as well as for business activities. The use of internet in organizations has made employees more efficient by providing improved and better communication channels, better workplaces in job design, and conditions of work. On the other hand, misuse of the internet in workplace has caused organization some setbacks resulting from lose of company integrity, availability, and confidentiality of system resources, low employee performance, legal liability, exposure of trade secrets, and other security concerns.

Unfortunately, many organizations in Nigeria are not able to measure or predict their employees productivity because little or no effort has been put in place to monitor their employees at workplace. Employee monitoring allows an organization to track employee activities and monitor worker engagement with workplace related tasks. An organization using employee monitoring software can measure productivity, track attendance, ensure security and collect proof of hours worked. Globally, new technologies are enabling more varied and pervasive monitoring and surveillance practices in the workplace. This monitoring is becoming increasingly intertwined with data collection as the basis for surveillance, performance evaluation, and proper management of organization system resources: hardware, software, data, and communication lines and networks. Organization system resources are now handled with better interconnected and interdependent facilities because internet connectivity is widely integrated into ambient or ubiquitous environments through intuitive interfaces or "smart"

interactions. Technology, though complex and modern, has become enablers of enablers (Laureate Education (Producer), 2012f), making people to rely extensively on technology. These technologies are enabled in a complex interconnectivity platform that seemingly opened up avenues for theft, fraud and other forms of security threats by offenders who might even come from within the organization (Bamrara, Singh, & Bhatt, 2013).

Also, organization enterprises are increasingly becoming competitive, with widespread cyberloafing and lawsuits. Through IT and Internet usage, employees may compromise an organization's confidential information, deliberately or inadvertently. Such concerns prompt companies to introduce employee monitoring to preserve the integrity, availability, and confidentiality of system resources, track employee performance, avoid legal liability, protect trade secrets, and address security concerns. Insider threat is believed to pose the greatest risk to their enterprise, and more than 40% report that the greatest security concern is employees accidentally jeopardizing security through data leaks or similar errors (CERT, 2013). Most office-based companies today are already using some sort of employee monitoring software systems. They implement a monitoring system to monitor: how employees behave toward clients, employee visiting time-wasting and unofficial websites during official time, block employees from visiting. Another important reason for installing an employee monitoring system is to prevent data leaks and employees from stealing sensitive information., track their company fleet of vehicles, and ensure policy implementation for sustainable productivity.

1.1 Problem Statement

Systems to generate accurate records on employee monitoring for measuring productivity statistics are virtually non-existent in Nigeria. Our purpose in this study was to identify the challenges of monitoring employees at workplace so as to predict their productivity and relevance in the Job for a sustainable economic development. The general IT problem postulated in this study was the poor monitoring of employees at workplace majorly due to lack of monitoring software and establishment of ethical practices and policies. The specific IT problem is that some managers and stakeholders of organizations lack strategies, policies, laws, guidelines, and value system for monitoring employees for sustainable economic development.

1.2 Research Question

What are monitoring systems and strategies used by stakeholders to effectively monitor employees IT and internet usage for sustainable economic development?

2. Literature Review

2.1 Monitoring IT and Internet Usage of Employees

This section provides a review of professional and academic literature relevant to employee monitoring for sustainable economic development. Monitoring employee at workplace is basically to secure organization system resources: hardware, software, data, and communication lines and networks and preserve the integrity, availability, and confidentiality of system resources. It is also to track employee performance, avoid legal liability, protect trade secrets, and address security concerns. Employee monitoring is good. However employee monitoring are becoming complex, dynamic and psychological. Companies are struggling to keep up with new technologies, because perimeter defences, control over devices, employee's adherence to policies, control over policy enforcement, and enterprise definitions are no longer reliable. This is because, as in reality, there are no perimeter boundaries, but all monitoring and security platforms are complex, dynamic and psychological (Thompson, 2013).

Employee monitoring has been defined as a system that allows an organization to track employee activities and secure worker engagement with workplace related tasks so as to measure productivity, track attendance, ensure security and collect proof of hours worked (Bejtlich, 2004; Moussa, 2015). Network Security Monitoring defines the strategic monitoring of network traffic to assist in the detection and validation of intrusions (Bejtlich, 2004). Organization productivity has been defined from a multiple perspectives (Narain, Gupta, & Ojha, 2014) and with a holistic approach that expands beyond the technology and technical security (Perez, Branch, & Kuofie, 2014), to comprise the environment, the technology, and the employee (Stallings & Brown, 2012; Taylor & Robinson, 2015). Significant amount of empirical researches point to the fact that employees appear to be the most important links to both the economic productivity and information security of any organization, and invariably constitute the highest risk to low productivity, information security measures and information integrity of any organization (Stallings & Brown, 2012). This is because of the differences in employee behaviour regarding the intent to implement monitoring or administrative policies (Komatsu, Takagi, & Takemura, 2013).

Technology: company websites, emails, devices, internet, phones, voicemails, locations, etc., are simply enablers of enablers (Laureate Education (Producer), 2012f). It is important that employers and employees understand and get better sense of what technology was meant for, and try to focus on the psychology of the creators and users of the technology rather than on the technical details of how they work or what they are

designed to do. Sustainability of organization productivity is all about psychology, not technology (Cottrell, 2016). When the US wanted to lunch the first humans on the moon, they did not just get the technology, they understood both the technology and the problem. Company productivity does not end with technology, but understanding technology and the user problems are enough to solve the productivity and its sustainability problems. Even self-driving cars won't work until we change our roads and attitudes. According to Rahman and Badayai (2012), employee job performance refers to the appropriate use of technology, work productivity, as well as to the time spent in the office, attendance, and resignation rate. Organizations regulate Internet use, or website visits by their employee, through two regular ways: by restricting access to particular links, and by monitoring employee actions (Moussa, 2015). Employee monitoring is good to align workers' attitude for sustainable productivity.

2.2 Resent Statistics on Employee Abuse of Work Hour Time

Accurate records on employee monitoring for measuring productivity statistics are virtually non-existent in Nigeria. A few published records have been noted statistically on impact of employee monitoring on productivity. Nigeria is one of the countries where no adequate system monitoring of employees, especially in public and government organizations take place. Employees are often masters of their own, doing whatever thing they choose to do during office hours. These have great consequences on sustainability of Nigeria's economic productivity. Findings from a few researchers claimed that an insignificant number of organizations in Nigeria monitor the websites connections of their employees, while a significantly large percentage does not restrict usage of the internet and websites during work hours (Atinuke, & Titilope, 2015; NITDA, 2019; Yusuf & Metiboba, 2012). This is not a healthy situation for a sustainable economic development as organizations in Nigeria are unable to monitor unproductivity among employees accruing from evidential office time wasting resulting from misuse of internet and websites. This is the gap this study intends to fill.

In the contrary, the latest on workplace monitoring and surveillance employee statistics by American Management Association (AMA), claimed that during office time, 64% visit non-work related websites, 85% use their company email for personal reasons, 70% connect to pornographic website, 92 % perform personal stock trading, 37% constantly surf the internet, 30% watch sports online, 25% shopped online, and 46% actively look for a new job on the internet. Internet surfing on non-work related results in up to a 40% loss of productivity each year for American businesses, while only 15% of businesses have a social media policy despite widespread use and misuse of social media at workplace (AMA, 2019). This is demonstrated in Figure 1 below.

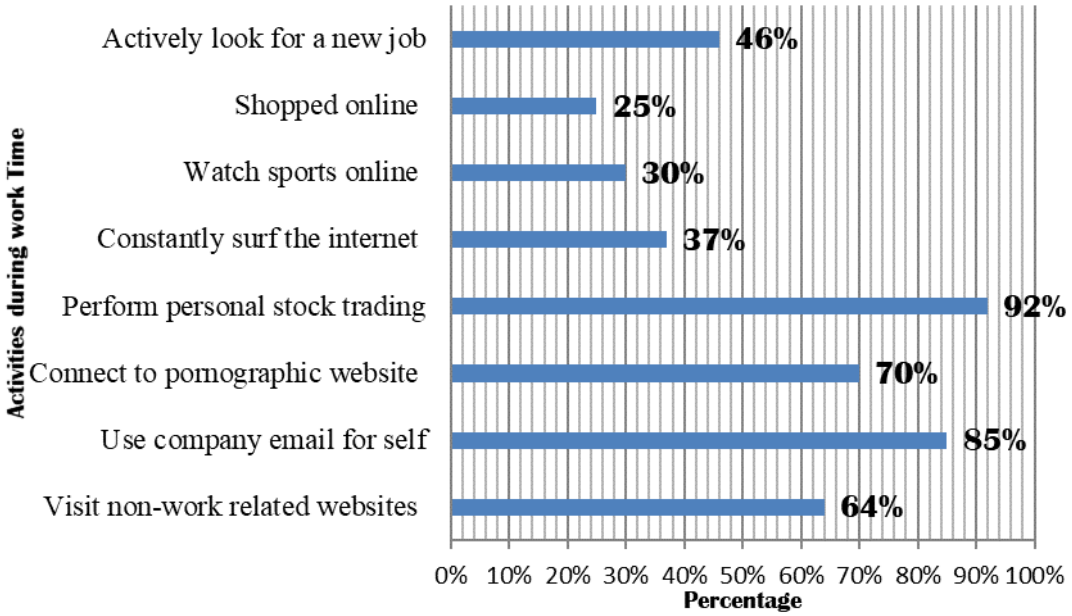

Figure 1. **Workplace Monitoring and Surveillance Employee Statistics.** AMA (2019).

Other employee monitoring and surveillance statistics are shown in the figures 2 and 3 below.

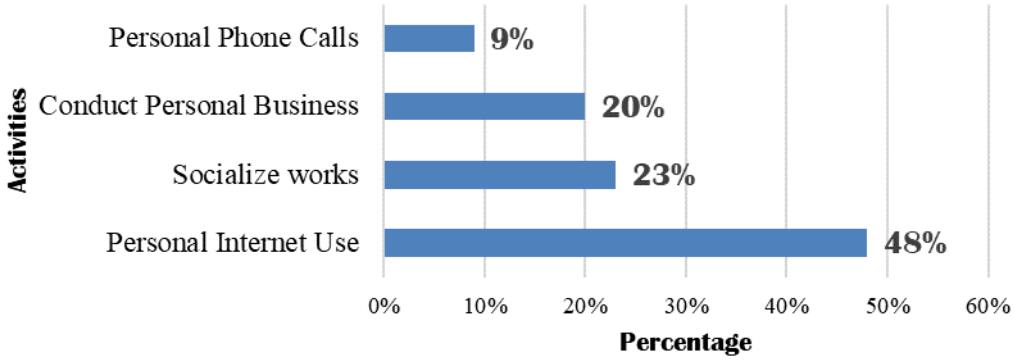

***Figure 2*. Leading Time Wasting Activities.** AMA (2019).

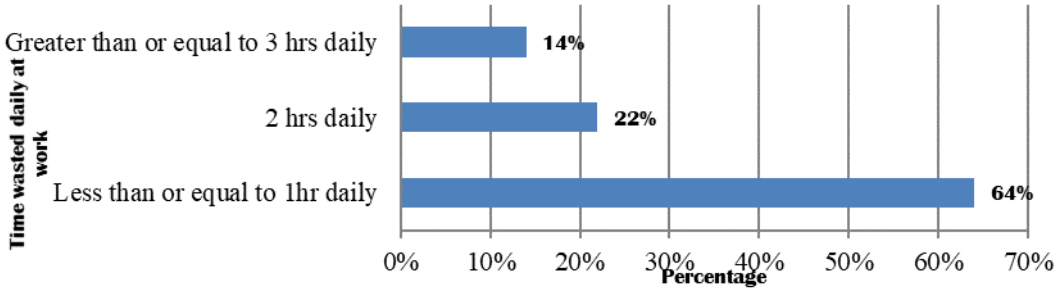

***Figure3*. Employee Time Wasting at Work.** AMA (2019).

According to AMA (2019), employers who have fired workers for e-mail misuse cite the following reasons: (a) violation of any company policy (64%), (b) inappropriate or offensive language (62%), excessive personal use (26%), breach of confidentiality rules (22%), and others (12%). Statistics also revealed that employers have fired workers for IT and Internet misuse under the following headings: (a) viewing, downloading, or uploading inappropriate/offensive content (84%), (b) violation of any company policy (48%), (c) excessive personal use (34%), and others (9%) (AMA, 2019).

Rather than monitoring their employees, a significant number of organizations in Nigeria prefer to block their employees from some specific websites the suspect employees go often during office work time. Results from Atinuke and Titilope (2015, p. 19), showed that "74.7% of the organizations surveyed block pornography sites, 59% blocked online gaming sites, 46.4% block social networking sites, 55.2% blocked downloading sites, 38.8% blocked yahoo messenger, 37.2% blocked Skype, 33.9% blocked online mail services sites, 36.1% blocked blog sites and 11.5% agreed to blocking other sites like competititor's sites, entertainment sites, online shopping sites, and many more". This is shown in figure 4. Below. These restrictions are necessary so as to aid employees' concentration at work, and to reduce traffic congestion on organisations servers, for sustainable productivity.

This finding agrees with the AMA survey of 2019 which showed that 64% visit non-work related websites (AMA, 2019).

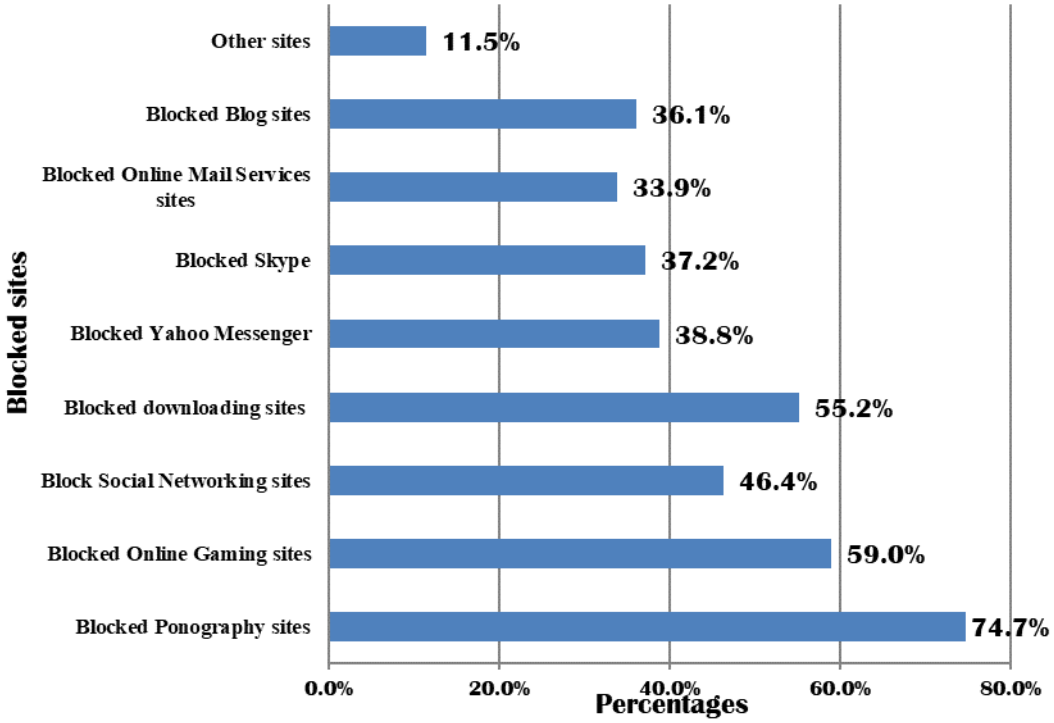

***Figure* 4 Blocked Sites (Nigeria)** Atinuke and Titilope (2015, p. 19)

Aside monitoring employees against wasting work time, it is also important to monitor employees to safeguard the company's information resources. This is because employees appear to be the most important links to the information security of any organization, and invariably constitutes the highest risk to the information security measures and information integrity of any organization (Stallings & Brown, 2012). Employees and users are often the weakest links in the security of a system. Many security breaches are caused by employees visiting unauthorized sites with unencrypted files left on unprotected systems, leading to losses of company income due to low productivity, litigations etc. Astakhova (2015) cited some eloquent figures from InfoWatch Analytical Center, that showed that out of 654 cases of leakage of confidential information that were recorded, 71% of them were employees of companies. Additionally, these threats are not effectively and efficiently mitigated (Silic & Back, 2014). Therefore determining what contributes to information insecurity through employee monitoring and securing employee workplace is also of paramount importance particularly in the implementation of policies and activities that mitigates threats to the organizations' data: confidentiality, integrity, and availability (Fenz, Heurix, Neubauer, & Pechstein, 2014).

3. Methodology

In this study, we adopted a narrative review approach to review significant information based on the, existing systems centred on employee workplace monitoring for sustainable productivity. We also reviewed, analysed and synthesized prior research findings. A narrative review is often adopted where analysis and synthesis of different and related research findings are required to draw holistic interpretations or conclusions based on the reviewers' own experience, existing theories, and models (Hill & Burrows, 2017). Our narrative methodology explicitly explained the methodological commitments of narrative inquiry by adopting the a search criteria that explicit included our review process, keywords and term identification, article identification, quality assessment, data extraction, and data synthesis. We also adopted methodological triangulation as recommended by Durif-Bruckert, et al. (2014), by using multiple sources of data to gain multiple perspectives for maximizing reliability and validation of data, in order to build coherent justification of data interpretation that relates to the study case or phenomenon. Methodological triangulation also ensured the reliability and validity of data, and justification of interpretations from the reviews.

4. Data Collection

We reviewed the research findings that are relevant and related to our study. Many of such findings came from peer-reviewed, and other related texts from the ProQuest databases, ScienceDirect, and scholar Google databases. We also used phrases and terms as key search words in the databases for related literature on employee IT and internet monitoring for predicting employee productivity in Nigeria. Such phrases and terms included employee

monitoring, monitoring ethics, employee website surfing and productivity, and many others. Our reviews incorporated 27 references. Ninety three percent (89%) of total references incorporated in the study is peer-reviewed, while (79%) are peer-reviewed journals that are within the last 5 years.

5. Ethical Issues in Employee Monitoring

Monitoring employees at workplace has been a controversial practice that is undeniably on the rise (AMA, 2019), with a grey area (Yerby, 2013). Employee monitoring is legal but there are some ethical considerations for its effectiveness (Yerby, 2013). Fundamental ethical issues in business include promoting conduct based on integrity and trust (Oster, & Seidel, 2019). However, there are more complex ethical issues that included accommodating diversity, empathetic decision-making, compliance and governance consistent with a company's core values such as diversity and the respectful workplace, decision-making issues, compliance and governance issues (Oster, & Seidel, 2019). Legally, it is believed that employee ultimately did not have a right to privacy for information on an employer-supplied computer systems, even when used at home (Collins, 2002; Yerby, 2013). But employees desire the true right to privacy they enjoy outside office work hours every day in their lives to be extended to their workplace too. Nevertheless, the reality is that when an employee is at work, the right to privacy is either non-existent, or significantly less than the one enjoyed after-hours (Yerby, 2013). Most people spend a great deal of their weekdays at their offices or job sites. This is why employees face ethical dilemmas. Several of these dilemmas pop up on a regular basis. However, employees can resolve common workplace dilemmas without losing their jobs or bringing harm to their employer by avoiding : conducting personal business on company time, taking credit for others' work, inappropriate and harassing behavior, stealing on the job, etc (Rafner & Thompson, 2019).

6. Discussions and Conclusions

Organizations can reap a lot of rewards from employee monitoring such as less wasted time without being intrusive, fewer errors, better employee insights, increased security and better management of resources including CIA system resources, more transparency, better delegation, and less administrative work. In spite of these advantages, monitoring IT and Internet usage of employees still has drawbacks. They include its effect on morale, increased stress, and perceived lack of privacy, higher turnover, and legal issues. Monitoring IT and Internet usage of employees is Legal and good for sustainable company productivity and economic development. Employee ultimately did not have a right to privacy for information on an employer-supplied computer systems, even when used at home (Collins, 2002; Yerby, 2013). There is an ongoing need in Nigeria for employee monitoring systems especially now that IT and Internet connectivity are becoming widely integrated into ambient or ubiquitous environments through intuitive interfaces or “smart” interactions. Organizations in Nigeria may experience tremendous innovations and economic development if all the benefits of monitoring IT and Internet usage of employees are appropriately harnessed. Therefore, findings from this study should have greater applicability to other developer organizations as well as other IT organizations that are technology dependent.

References

AMA (2019). The Latest on Workplace Monitoring and Surveillance. Retrieved May 13, 2019 from https://www.amanet.org/articles/the-latest-on-workplace-monitoring-and-surveillance/

Astakhova, L. V. (2015). Information security: Risks related to the cultural capital of personnel (Review). *Scientific and Technical Information Processing, 42*(2), 41-52. doi:10.3103/S0147688215020021

Atinuke, A .A., & Titilope, A. O. (2015). Internet Access, use and Monitoring Policies in Selected Organisations in Ibadan, Nigeria. *Global Journal of Management and Business Research: Administration and Management, 15*(11), 13-26.

Bamrara, A., Singh, G., & Bhatt, M. (2013). Cyber Attacks and Defense Strategies in India: An Empirical Assessment of Banking Sector. *International Journal of Cyber Criminology, 7*(1), 49-61

Bejtlich, R. (2004). What Is Network Security Monitoring? http://www.informit.com/articles/article.aspx?p=350391

Belmont Report (1979). *The Belmont Report: Ethical principles and guidelines for the protection of human subjects of research.* National Commission for the Protection of Human Subjects of Biomedical and Behavioral Research. Retrieved May11, 2019, from hhs.gov/ohrp/humansubjects/guidance/belmont.html

CERT (2013). CERT Insider Threat Team. *Unintentional Insider Threats: A Foundational Study* (CMU/SEI2013-TN-022). Software Engineering Institute, Carnegie Mellon University, May 2013. http://resources.sei.cmu.edu/library/asset-view.cfm?assetID=58744

Collins, Z. (2002). No expectation of privacy on company computer used at home. *The Computer & Internet Lawyer*, *19*(5), 35-37.

Cottrell, L. (2016). IoT problems are about psychology, not technology. Retrieved from http://www.tripwire.com/state-of-security/security-data-protection/iot/iot-problems-are-about-psychology-

not-technology/

Durif-Bruckert, C., Roux, P., Morelle, M., Mignotte, H., Faure, C., & Moumjid-Ferdjaoui, N. (2014).Shared decision-making in medical encounters regarding breast cancer treatment: the contribution of methodological triangulation. *European Journal of Cancer Care, 24*(4), 461-472. doi:10.1111/ecc.12214 executives in Lagos state, Nigeria. *Greener Journal of Business and Management*

Fenz, S., Heurix, J., Neubauer, T., & Pechstein, F. (2014). Current challenges in information security risk management. *Information Management & Computer Security, 22*(5), 430-410. doi:10.1108/imcs-07-2013-0053

Hill, C., & Burrows, G. (2017). New voices: The usefulness of a narrative approach to social work research. *Qualitative Social Work: Research and Practice, 16*(2), 273-288. doi:10.1177/1473325017689966

Oster, K. V., & Seidel, M. (2019). List of Ethical Issues in Business. Retrieved April 16, 2019 from https://smallbusiness.chron.com/list-ethical-issues-business-55223.html

Komatsu, A., Takagi, D., & Takemura, T. (2013). Human aspects of information security. *Information Management & Computer Security, 21*(1), 5-15. doi:10.1108/09685221311314383

Laureate Education (Producer). (2012f). CIO interview: Setting policies [Video file]. Retrieved from https://class.waldenu.edu

Moussa, M. (2015). Monitoring Employee Behavior Through the Use of Technology and Issues of Employee Privacy in America. *SAGE Open, 5*(2), 1-13. doi:10.1177/2158244015580168

Narain, S. A., Gupta, M. P., & Ojha, A. (2014). Identifying factors of "organizational information security management. *Journal of Enterprise Information Management, 27(*5), 667-644. doi:10.1108/jeim-07-2013-0052

National Information Technology Development Agency (NITDA) (2019). Framework and guidelines for public internet access(PIA). 1-14.

Perez, R. G., Branch, R., & Kuofie, M. (2014). EOFISI Model as a Predictive Tool to Favor Smaller Gaps on the Information Security Implementations. *Journal of Information Technology and Economic Development, 5*(1), 1-20.

Rafner, D., & Thompson, J. (2019). Common Ethical Workplace Dilemmas. Retrieved April 20, 2019 from https://smallbusiness.chron.com/common-ethical-workplace-dilemmas-748.html

Rahman, A., & Badayai, A. (2012). A Theoretical Framework and Analytical Discussion on Uncongenial Physical Workplace Environment and Job Performance among Workers in Industrial Sectors. *Procedia - Social and Behavioral Sciences 42*(1), 486 – 495. doi: 10.1016/j.sbspro.2012.04.214

Silic, M., & Back, A. (2014). Information security: Critical review and future directions for research. *Information Management & Computer Security, 22*(3), 308-279. doi:10.1108/IMCS-05-2013-0041

Stallings, W., & Brown, L. (2012). Computer security: Principles and practice (2nd ed.). Upper Saddle River, NJ: Prentice Hall.

Taylor, R. G., & Robinson, S. L. (2015). An information system security breach at First Freedom Credit Union 1: what goes in must come out. *Journal of the International Academy for Case Studies, 21*(1), 131-138.

Thompson, H. (2013). The human element of information security. *Security & Privacy, IEEE, 11*(1), 32-35.

Yerby, J. (2013). Legal and ethical issues of employee monitoring. *Online Journal of Applied Knowledge Management, 1*(2). 44-55.

Yusuf, N., & Metiboba, S. (2012). Work Environment and Job Attitude among Employees in a Nigerian Work Organization. *Journal of Sustainable Society, 1*(2), 36-43.